

**Office of the
Attorney General**

Internet Safety



AUGUST 2005

LAWRENCE WASDEN
Attorney General
Statehouse
Boise, ID 83720-0010
www.ag.idaho.gov



State of Idaho Office of Attorney General Lawrence Wasden

Dear Fellow Idahoan:

The Internet is an exciting tool that puts vast amounts of information at your fingertips. With the click of a mouse, you can buy airline tickets, use research tools, chat with friends or play interactive games.

But there are also risks on the Internet, so it's important to be cyber-smart and make your experience online a safe one. It is critically important that parents supervise their children's Internet use. As we've seen all too often, trusting children are particularly vulnerable to sexual predators and other cyber-criminals.

When you go online, keep in mind your personal and financial safety, security and privacy. You should also take a cautious approach to online "business opportunities" and be wary of Internet scams and computer viruses.

My office has prepared this publication to help you safely enjoy the Internet. I hope you find it helpful.

LAWRENCE G. WASDEN
Attorney General

Table Of Contents

SAFETY AND SECURITY	1
SHOPPING ONLINE	1
USE A SECURE BROWSER	1
SHOP WITH COMPANIES YOU KNOW	2
KEEP A PAPER COPY OF YOUR PURCHASE	3
PASSWORDS.....	4
E-MAIL	5
ADVANCE FEE SCAM.....	5
“PHISHING” OR VERIFICATION SCAM	8
INTERNATIONAL LOTTERY SCAM.....	10
“SPAM”	11
CHILD SAFETY	13
PRIVACY	15
PERSONAL INFORMATION	15
PRIVACY POLICIES.....	15
SITE SECURITY	16
COOKIES	16
PHARMING	17
SPYWARE	18
ONLINE BUSINESS OPPORTUNITIES	20
INTERNET BUSINESS SCAMS.....	21
COMPUTER VIRUSES	23
WHAT IS A VIRUS?.....	23
HOW DOES A COMPUTER GET A VIRUS?	23
HOW DO YOU REMOVE A VIRUS?	24
PREVENTIVE MAINTENANCE	25

APPENDIX A	25
ONLINE RESOURCES.....	25
APPENDIX B	28
GLOSSARY	28

SAFETY AND SECURITY

The Internet has opened a new world for many people. Information, communication and shopping at distant retail outlets are readily available. Yet there are serious risks associated with e-mail, browsing, and doing business online.

One of the greatest risks is that the Internet is an anonymous place with no face-to-face contact. Thieves and predators take advantage of this anonymity and pretend to be someone other than who they really are.

These tips can help ensure your safety on the Internet.

SHOPPING ONLINE

Use a secure browser

A browser is the software you use to explore the Internet. Your browser should comply with industry security standards, such as Secure Electronic Transaction (SET). These standards encrypt or scramble the purchase information you send over the Internet, ensuring the security of your transaction. Most computers come with a secure browser already installed.

You can determine whether your browser is secure from your web browser window. Select the “HELP” menu option and then select “ABOUT.” The information pop-up window will display the encryption level.

If you do not have a secure browser, there are many to choose from. The most common browsers include Netscape Navigator and Microsoft Internet Explorer. You can download these browsers free from the Internet.

When shopping online, it is also very important that you are buying from a secure web site. See “Site Security” on page 16 for more information.

Shop with companies you know

Anyone can set up a business under almost any name on the Internet. If you are not familiar with a business, look for a physical address, a phone number and an e-mail address. Contact the business and ask for a brochure or catalog of merchandise and services. Request a copy of the business’s refund and return policy. Contact the Better Business Bureau and the Consumer Protection Agency in the business’s home state to find out what kind of track record the business has. If you are purchasing an item from an Internet auction, check the seller’s feedback rating.

Before you make a purchase, make sure that you know what you are paying for. Review the description, price information, and any limitations on purchases (for example goods may not be available for delivery outside of the country; there may be minimum quantities that must be ordered; etc.)

Review the fine print and look for words such as “refurbished,” “close-out,” “discontinued” or “off-brand.”

Check whether the price is listed in U.S. dollars or another currency. Review the requirements for taxes or duty on purchases, as well as postage costs and shipping and handling charges.

Review the company’s privacy policy. The policy should state what information is collected, how it will be used, and whether the information will be shared with others.

If you have questions about the item or any of the charges or policies, e-mail or phone the seller.

Keep a paper copy of your purchase

When you order something over the Internet, keep a printed copy of your purchase order, receipt, or confirmation number. A paper record will help resolve problems with your purchase.

If you pay by credit card or debit card, your transaction is protected under the Fair Credit Billing Act. This federal law gives consumers the right to dispute charges under certain circumstances and to temporarily withhold payment on the disputed charges while an investigation is done. If you pay by credit card or debit card, there are protections for unauthorized payments under the federal Electronic Fund Transfer Act. For more information on

these laws, contact the Attorney General's Consumer Protection Unit.

If you are purchasing an item from an Internet auction and the seller does not accept credit cards, consider using an escrow service. If the seller only accepts cashier's checks or money orders, decide whether you are willing to take the risk of sending your money before you receive the product. Be sure to take steps to protect your privacy – do not give out personal and sensitive information such as your Social Security number, driver's license number or bank account number.

The federal Mail or Telephone Order Merchandise Rule also covers purchases made over the Internet. Unless otherwise indicated, this rule requires that the merchandise must be delivered within 30 days. The company must notify you if the merchandise cannot be delivered within that time frame.

PASSWORDS

Many websites require you to register and create a password for future access. When creating a password, the National Crime Prevention Council suggests you mix numbers with upper and lowercase letters, or use a word that is not found in the dictionary. Avoid using personally identifiable information such as your phone number, birth date, or a portion of your Social Security number.

It is also a good idea to use a different password for each Internet site you use.

Keep your passwords in a secure place. Do not have your computer “remember” your passwords unless you are the only person with access to your computer.

E-MAIL

The major difference between e-mail and the old fashioned kind of mail is privacy. Think of e-mail as a postcard rather than a sealed letter. Your e-mail can be intercepted, either intentionally or unintentionally, at many points along its path. So while e-mail is a great way to stay in touch, it might not be a great way to send confidential information.

Criminals are increasingly using e-mail as a tool for fraud. Some of the common scams are:

1. Advance Fee Scam
2. “Phishing” or Verification Scam
3. International Lottery Scam

Advance Fee Scam

Advance Fee Scams include requests for your personal bank account information or asking you to pay an advance fee for taxes, attorney fees, and other transactional costs in order to receive a benefit or money. Advance Fee scams include:

1. Disbursement of money from wills
2. Contract fraud
3. Real estate transactions
4. Conversion of currency
5. Transfer of funds
6. Sale of crude oil at below market prices

One common example is the “Nigerian Money Scam.” In this scam, you’ll receive an urgent request to help someone get his or her money out of Nigeria (or another country). You may receive official looking documents to support the request, stating that it is from an official representing a foreign government or agency. These requests may appear to be personally addressed to you, but in fact they are sent out in mass mailings. They’ll offer you a large amount of money if they can move the money through your bank account. Of course, they’ll ask for your account number. If they get it, they will empty the account. They may also ask you to pay in advance for taxes, attorney fees, and other transactional costs in order to “transfer” the money into your account.

If you receive e-mails (or faxes or letters) similar to either of these scams:

1. Do not respond.
2. Destroy the e-mail, fax or letter.

3. If you have become a victim of this scam - that is, if you have provided your bank account number or other personally identifying information or if you have lost money - notify the United States Secret Service.

Write to: U.S. Secret Service, Financial Crimes Division, 245 Murray Drive, Building 410, Washington, DC 20223. E-mail complaints can be sent to the Secret Service at 419.fcd@uss.s.treas.gov. When you contact the Secret Service, be sure to include a copy of the original e-mail. You can also call the national office at 202-406-5708 or the Boise office at 208-334-1403.

Another example of advance fee scams involves overpayment of a purchase.

You may become a target of this scam if you are selling an item over the Internet. The “purchaser” will “mistakenly” send you a check for more than the purchase price and ask you to send back the difference. The problem is that the check the “purchaser” sends you is counterfeit. You will lose the money you sent back and the amount of the counterfeit check.

To avoid being victim to an overpayment scam, you should:

1. Confirm the buyer’s name, address and telephone number.

2. Refuse to accept a check for more than your selling price. If the buyer sends a check over the amount due, return the check and ask for a check in the correct amount. Do not send the merchandise until you receive the correct amount.
3. Consider an alternative source of payment such as an escrow service or online payment service. Be sure to verify that the escrow service or online payment service is legitimate by reviewing its website; reviewing its policies and terms and conditions; calling its customer service line; and checking with the Better Business Bureau or the Attorney General's Consumer Protection Unit to see if there are complaints against the service.
4. Not wire funds back to the buyer.

“Phishing” or Verification Scam

If you are a target of this scam, you will receive an e-mail or pop-up message that appears to be from a trusted company. These e-mails and messages often contain color graphics and look just like the company's Internet site.



The e-mail or message will indicate that the company needs to verify information for its records and will ask you to provide your credit card number, automatic teller PIN number, Social Security number and/or other confidential information. This scam is also known as “phishing.”

The Attorney General's Office has seen fraudulent e-mails that appear to be from well-known companies including PayPal, E-Bay and MBNA, a major credit card company. These e-mails are fraudulent. They are not from these companies. The sender is trying to get information that can be used to steal your identity or your money.

The companies with whom you do business already have the information they need. Legitimate companies will not contact you by e-mail to verify information you have already provided.

If you receive e-mails (or faxes, letters or phone calls) similar to this scam you should:

1. NEVER PROVIDE THE INFORMATION REQUESTED.
2. Find the e-mail address of the real company and forward the e-mail to the company's security or fraud department. Or, you can call the company using a telephone number you know to be genuine.
3. Delete the e-mail from your computer. Do not click on any link in a suspicious e-mail. Log on to website accounts by opening a new browser window and typing the URL website address directly into the address bar. Do not "copy and paste" the URL link from the message into your address bar.

4. Only use secure websites to submit sensitive or personal information. Look for the lock  or key  icon at the bottom of your browser and a URL with an address that begins with “https.”
5. Review credit card and bank account statements regularly to determine whether there are any unauthorized charges.
6. Maintain up-to-date anti-virus software. Some phishing e-mails contain viruses. Consider installing firewall protection.

You can report phishing to the Federal Trade Commission (FTC). Forward the e-mail to spam@uce.gov. If you believe that you have been injured (lost money, had your identity stolen, etc.) by phishing, you can file a complaint with the FTC at www.ftc.gov.

International Lottery Scam

Another common scam is the International Lottery Scam. This scam uses e-mail, direct mail and the telephone to entice you to purchase chances in international lotteries. When you send money to purchase a lottery ticket, many scam operators do not buy the promised tickets. Instead, they simply keep the money for themselves. Other operators will buy some tickets and keep any winnings for themselves. Operators will often make unauthorized withdrawals

from your bank account or make unauthorized charges to your credit card.

If you purchase a ticket from one of these scam operators, there's a good chance they will put your name on a list of potential victims and sell it to fraudulent telemarketers and other scammers who will try to sell you other bogus offers for lottery and "investment opportunities."

If you receive a solicitation to purchase international lottery tickets:

1. Do not respond to the solicitation.
2. If the solicitation is by telephone, file a complaint with the Attorney General's Consumer Protection Unit.
3. If the solicitation is by direct mail, give the letter to your local postmaster.
4. If the solicitation is by e-mail, delete the e-mail.

"Spam"

"Spam" is the e-mail version of junk mail: unwanted e-mail messages from people you do not know seeking to sell you a product or service. Spammers get your e-mail from places such as websites, chat rooms, membership directories, and newsgroup postings.

To reduce the amount of spam you receive, you should:

1. Consider having two e-mail addresses. One e-mail address can be used for personal messages and the other address can be used for newsgroups and other purposes. Or, one address can be used as your “permanent” e-mail address and the other can be considered “disposable.”
2. Review privacy policies before submitting your e-mail address to a website. Some websites will allow you to “opt out” of receiving offers or e-mails from another business or having your address sold to another business.
3. Use an e-mail filter. Your e-mail account may have a tool to filter out potential spam or a method of channeling spam into a bulk e-mail folder.

The Federal “CAN-SPAM” Act of 2003 requires spammers to allow you to “opt out” from receiving future e-mails. Many people, however, report that they receive additional e-mails from other spammers after they ask to be removed from one spammer’s list. You can report spammers that do not honor your “opt out” request to the Federal Trade Commission (FTC) by filling out a complaint form at www.ftc.gov.

You can also forward unwanted or deceptive messages to the FTC at spam@ftc.gov or complain to the spammer’s Internet service provider. Be sure to include

a copy of the message and header information and state that you are complaining about spam.

CHILD SAFETY

The Internet offers great educational and entertainment opportunities for children. It also offers great danger, most notably from sexual predators.

Because of their trusting nature, children are particularly vulnerable in Internet “chat rooms.” Child predators know this and often pose as children in order to gain the trust and confidence of a potential victim.

There have been many cases in Idaho in which a child has been lured to meet with an “on line friend” who turns out to be an adult and a sex offender.

Here are some Internet safety tips for parents and kids:

1. Communicate. Talk to your child about the potential hazards of the Internet. Regularly have them show you the websites they visit. Get to know their online friends just as you would their regular friends.
2. Keep the computer in a central room. It’s harder to keep a secret when parents can regularly see what their child is doing online.
3. Use parental controls and/or blocking software. Most Internet service providers (ISP) provide

graduated levels of parental controls that block access to certain adult-oriented sites. Many software packages on the market are also effective.

4. Keep track of the websites viewed by your children by checking the web browser history files and cache.
5. Maintain access to your child's account and randomly check e-mail. At first, you may feel that you are invading your child's privacy. Think of it another way. If your child received letters or phone calls from a stranger, would you ask who that person is?
6. Teach your children not to give out any information about themselves. Predators can use seemingly insignificant information (for example, hobbies, school or age) to identify and locate a child.
7. Report inappropriate online activities. Notify the police immediately if an online contact tries to set up a meeting with your child.
8. Do not allow your children to use chat rooms. Even seemingly safe "kids" chat rooms can be dangerous.

The National Center for Missing and Exploited Children has assembled a very useful, informative and fun

Internet safety program for parents and kids. You'll find it at www.netsmartz.org.

PRIVACY

Some Internet sites may share information about you with affiliates. They may also sell your personal information. Before you provide information to an Internet site, decide what personal information you want to keep private and what information you are willing to have released.

If you are concerned about privacy, consider these tips.

Personal information

Never give out your Social Security or driver's license numbers over the Internet.

Do not disclose other personal information such as your address, telephone number, or e-mail address, unless you have researched a company's privacy policy and know the company has a good reputation. Even then, find out exactly what information is being collected and how the company will use it. Many companies are joined with other affiliates or partners that have full access to their customer files.



Teach your children not to give out personal or family information online.

Privacy policies

Many companies post their privacy policy on their Internet site. If you are unable to locate a company's privacy policy, send an e-mail or written request for a copy.

Read the policy carefully before you give a site your personal information. Check to see if the company will transfer the personal information you provide to affiliates or other businesses or organizations.

Site security

Before conducting any transactions online, verify that the company's website is secure. A secure website means the company has taken precautions to ensure that others cannot intercept information. You will **always** see a padlock  or key  icon in the lower corner of the screen when a site is secure.

Make sure your browser has the most up-to-date encryption capabilities. Also, look for the phrase "https:" in the URL.

Cookies

"Cookies" are pieces of data an Internet site places on the hard drive of your computer. Cookies originate from the sites you visit. In effect, cookies record your digital comings and goings.

Cookies can only be read by the web server that originated the cookie. Other web servers cannot intercept cookies.

Cookies perform many functions, including serving as navigational tools or as a means for searching the Internet. Cookies also keep track of goods you intend to purchase but set aside while you finish shopping a website. Cookies can collect and transfer a great deal of information about you and your interests every time you go online — even when you don't go to the checkout or log off.

Both Netscape Navigator and Microsoft browsers allow you to block cookies or prompt you before a cookie is downloaded to your computer. However, by disallowing cookies, you may reduce or even eliminate your browsing options in many websites.



Visit www.cookiecentral.com for more information about cookies, including how to remove cookies from your browser completely.

Pharming

“Pharming” involves the redirection of an Internet user from a legitimate commercial website to a bogus website. “Pharmers” set up bogus sites and shuttle users from legitimate websites by altering the domain name system or transmitting a virus.

The bogus website will look the same as the legitimate website. When you enter your login name or identification and password, “pharmers” obtain the information for their own use. This can occur even when you type the correct URL.

You can take steps to avoid being a victim of pharming:

1. Maintain up-to-date antivirus software.
2. Consider installing anti-spyware software and firewalls.
3. Be careful when entering personal or sensitive information into a website. Be sure to look for the lock  or key  icon at the bottom of your browser.
4. Review websites closely. If the website has changed since your last visit, be suspicious. If you have any doubt about the website, do not use it.

Spyware

Spyware is software that is installed on your computer without your consent. Spyware monitors or controls your computer use without your knowledge. It is also called “adware.” Spyware is often used to send you pop-up advertisements, direct you to certain websites, monitor your internet surfing, and even to record your keystrokes. Spyware can lead to identity theft.

You may have spyware installed on your computer if you experience problems such as numerous pop-up advertisements; a browser that takes you to sites other than those that you typed into the address bar; sudden or repeated change in your home page; new or unexpected toolbars or icons at the bottom of your computer screen; keys that no longer work; random error messages; or slow performance when opening programs or saving files.

To prevent the installation of spyware:

1. Keep your operating system and browser software up-to-date.
2. Do not download software from sites you do not know and trust.
3. Do not install software without knowing exactly what it is. Read the end-user license agreement before you install software.
4. Set your browser security setting to a high level and keep it updated.
5. Do not click on links within pop-up windows. Close pop-up windows only by clicking the “x” icon in the title bar.
6. Do not click on links in spam that offers “anti-spyware” software. Many of these are fraudulent and actually install spyware onto your computer.

7. Consider installing a firewall.

ONLINE BUSINESS OPPORTUNITIES

The Internet also offers many business opportunities. If you find one that interests you, be sure to thoroughly investigate the company before you sign up.

The Federal Trade Commission (FTC) advises that you:

- Understand that seminar “consultants” are often in business to sell you a business opportunity rather than to teach you Internet basics. In some cases, they may seek to exploit your lack of experience with computers or the Internet.
- Investigate all earnings claims. Talk to others who have purchased the opportunity to see whether their experience supports the company’s claims.
- Demand to see the company’s claims and promises in writing.
- Ask for a disclosure document. The FTC Franchise Rule requires most business opportunities to provide a disclosure document. The disclosure document should contain detailed information to help you compare one business with another.

- Contact your local Better Business Bureau and/or the consumer protection agency in the state where the business is located. Ask if complaints have been filed against the business.

Internet Business Scams

The Internet has been used to perpetrate a variety of scams. Consumers have complained about some of the following items relating to the Internet:

- Auctions: You receive an item that is not what was represented, less valuable than promised, or you receive nothing at all. Sometimes sellers fail to deliver in a timely manner or fail to disclose all the relevant information about the product or terms of sale.
- Internet access services: You cash a check you received from a business and are then locked into a long-term contract for Internet access or another web service, with penalties for cancellation or early termination.
- Work at home offers: You are offered the chance to earn “big bucks” by working at home or starting a new business. In fact, you will work many hours without pay and you may have to pay costs up front.

- Advance fee loans: You are offered loans for a fee, regardless of your past credit history. These offers are often a way to collect money without providing legitimate loans.
- General merchandise sales: You do not receive the merchandise, it is not the value or quality promised or you are charged extra fees.
- Travel Offers: You are offered luxury trips at bargain prices and receive lower quality accommodations and services or none at all, or you are charged extra fees.
- Pyramids, multilevel marketing and chain letters: You are offered the chance to make money through selling products and services and bringing others into the program. Neither you nor the people who brought you into the program make any money. Many of these programs are illegal.
- Weight loss claims: You are offered a “miracle” treatment, but instead are sold worthless or sometimes even dangerous products.
- Credit repair offers: You are offered the chance to erase accurate negative information from your credit records. These offers are false.

- **Adult entertainment offers:** You are offered the chance to view adult images “free” if you share your credit card number to prove you are over 18 years of age. Or, you are offered “free” access to adult material by downloading a viewer or dialer computer program. You should expect to have charges placed on your credit card. You may later receive international long distance charges on your phone bill for international modem dialing.
- **Web cramming:** You are offered a free website for a trial period, and are later charged on your phone bill or receive invoices for the websites.
- **Investment opportunities:** You will be offered a “ground floor opportunity” or promised big profits in a short time. You will be charged advance fees or receive no legitimate investment at all. Be wary of investments that state that they are “IRS approved” or are tax-free and confidential.

COMPUTER VIRUSES

What is a virus?

A virus is a file or program planted in your computer without your knowledge. Its purpose is to damage files and disrupt your computer.

How does a computer get a virus?

Most viruses are spread by file attachments sent through e-mail or on a floppy disk, CD, DVD or removable media. When you use an infected file on your computer, the virus copies itself onto your hard drive. Some viruses strike and cause problems immediately. Others remain inactive until a specific program is used or until a certain date occurs.

Viruses spread very rapidly. If you find that your computer has been infected, you should assume that every file and computer that you have used is also infected. Failure to scan and disinfect every disk and computer will almost guarantee that the virus will re-infect your computer or network.

How do you remove a virus?

Typically, viruses can be removed only by using anti-virus software or by re-formatting the infected hard drive. If you suspect that your computer is infected with a virus, you will need to research anti-virus software and purchase the appropriate package. Some popular brand names include Norton, McAfee and Kapersky.

Once your anti-virus software is installed, there are options to restore or repair damaged information and remove any harmful files that were saved to your computer. There is a chance, however, that you may have lost data that cannot be retrieved. You can reduce this risk by frequently making “back ups” of your personal data.

Preventive Maintenance

- Make sure that all computers have anti-virus software installed.
- Update your virus definition files from the anti-virus software manufacturer's website at least once a week.
- Scan e-mail attachments before you open them and scan floppy disks before you allow them on your computer. Do not download files sent to you by people you do not know.
- "Back up" your personal data frequently and on a regular schedule. Make back ups on CD media, Zip drive or floppy disks, not on your main hard drive.

APPENDIX A

Online Resources

You'll find more information about Internet safety at these Internet sites.

www.ag.idaho.gov

This publication is available on the Attorney General's website. The Attorney General's site also contains publications on other consumer protection issues.

www.fraud.org

The National Consumers League provides advice about the Internet and Internet fraud. You can report suspected scams with an online form.

www.netismartz.org

The National Center for Missing & Exploited Children provides child safety information for parents and children.

www.consumer.gov

This federal agency website provides consumer information and publications.

www.pueblo.gsa.gov

The Consumer's Resource Handbook, available on this federal government website, lists local, state and federal agencies, major trade associations, and consumer groups.

www.bbbonline.org

The Better Business Bureau reliability program for participating online merchants links to a central BBB site for reports about businesses and information on how to contact individual BBB's across the United States.

www.ftc.gov

The Federal Trade Commission offers online pamphlets relating to Internet shopping, Internet

and e-mail scams, online business opportunities, and additional consumer topics. The FTC also offers an online complaint form for consumers who encounter problems within the marketplace.

APPENDIX B

Glossary

The Internet has its own terminology. Here are a few key terms.

Adware – Adware is software that is installed on your computer without your consent. Adware monitors or controls your computer use without your knowledge. It is also called “spyware.”

Attachment – A file that is sent with an e-mail message.

Browser – A browser is the program that requests Internet documents from a server and displays these documents on your screen. More than likely the program you are using at home is a web browser. Popular browsers include Netscape Navigator, Lynx, and Microsoft Internet Explorer.

Cookie – Small files placed on the hard drive of your computer by some websites that you visit.

Download – Copying files from the Internet to your computer.

E-mail or electronic mail – Messages, similar to letters, sent or received through the Internet. E-mail can be addressed to one person or a group of people.

Encryption – An algorithm, used to scramble data, which makes the data unreadable to everyone except the recipient. E-commerce sites often use encryption to secure credit card data. Secure websites use encryption.

Hyperlink – An electronic connection that automatically takes you from one website to another. For example, the Attorney General’s website provides a hyperlink to the Consumer Protection page on its site.

Internet commerce (e-commerce) – Buying and selling goods and services over the Internet. Transactions take place between businesses and consumers through a computer network.

Modem – A hardware device that uses telephone or cable lines to connect your computer to the Internet or allows you to communicate with other computers.

Pharming – “Pharming” involves the redirection of an Internet user from a legitimate commercial website to a bogus website. “Pharmers” set up bogus sites and shuttle users from legitimate websites by altering the domain name system or transmitting a virus.

Phishing – “Phishing” is a scam intended to obtain your passwords and other personal and confidential information that can be used to steal your identity. “Phishing” is conducted by fraudulently sending an e-mail that appears to be from a legitimate business. Usually the e-mail will contain a link to a fake (but legitimate-looking) Internet site. If you log on to the

fraudulent site, the “phishers” will capture your user ID and password enabling them to access your account.

Search engine – A program that searches the Internet for specified keywords or phrases and returns a list of the documents containing the keywords or phrases. Google, Excite, and Yahoo are some well-known search engines.

Spam – “Spam” is the e-mail version of junk mail: unwanted e-mail messages from people you do not know seeking to sell you a product or service.

Spyware – Spyware is software that is installed on your computer without your consent. Spyware monitors or controls your computer use without your knowledge. It is also called “adware.”

URL – Uniform Resource Locator. This is the address of a specific website. You can type the URL into your computer to take you directly to that site on the Internet. For example, www.ag.idaho.gov is the URL address for the Office of the Attorney General.

Virus – A file planted in your computer that can damage files and disrupt your computer.

Website – An Internet destination where you can look at and retrieve data.

Funds collected by the Attorney General's Consumer Protection Unit as the result of enforcement actions paid for this pamphlet. No tax monies were used to pay for this publication.

The Consumer Protection Unit enforces Idaho's consumer protection laws, provides information to the public on consumer issues, and offers an informal mediation process for individual consumer complaints.

If you have a consumer problem or question, please call 208-334-2424 or in-state toll-free 1-800-432-3545. TDD access and Language Line translation services are available. The Attorney General's web site is available at www.ag.idaho.gov.